**Proceedings of the 2000 IEEE
Workshop on Information Assurance and Security
United States Military Academy, West Point, NY, 6-7 June, 2000**

Performance Modeling of AFATDS and Other Applications: Implications for Information Assurance and Security

John R. James, Dan Ragsdale, Joseph Schafer, Tim Presby

ABSTRACT: Planning of complex activities is a deliberative process and automation support for re-planning activities should provide for cognitive modeling of the planning process. This paper takes the position that the cognitive model should contain details of the domain being supported and, especially for support of on-line re-planning, knowledge of the system implementation architecture – including performance modeling of the implementation architecture. We discuss these thoughts in some detail and provide an overview of a test bed framework being implemented to perform experiments on the validity of this approach. In particular, we are interested in creating analysis tools that apply metrics to sensed data to assist in determining when a re-planning activity is required and in prioritizing re-planning activities. The framework is intended to support experiments with military decision making and, in particular, with re-planning activities that support execution of a military Operation Order (OPORD). One of the products often created during OPORD preparation is the commander's Synchronization Matrix (also know as an Execution Matrix) to support coordination of operational activities by different units. Likewise during OPORD execution, if a synchronization matrix exists, monitoring of the degree to which actual events correspond to those entered in the synchronization matrix provides an effective approach to estimating whether the commander's Concept of the Operation is being followed. We are investigating use of a new simulation tool to accumulate information at the message-packet-level and perform analysis at the network-application-level. We discuss use of this framework for pattern recognition of activities distributed in time and space. Finally, we assert that this level of detail is required to enable assessment of the information assurance situation to support evaluation of risks, as well as implementation and application of metrics for analysis of alternatives for reacting to attacks and monitoring of the selected alternatives.
KEY WORDS: metrics, performance modeling, distributed computing, latency, cognitive modeling, pattern recognition

I. INTRODUCTION

Information Operations is a new area of responsibility for military units and a new area of interest for military institutions. This interest is motivated by the realization that increased reliance on benefits accruing from expanded use of information system technologies creates *opportunities* for offensive information operations capabilities and *vulnerabilities* for defensive information operations capabilities. Commercial enterprises face similar opportunities/vulnerabilities in the electronic commerce area. Information Operations are characterized by both the wide range of target/defended system dynamics as well as by the increased complexity of interaction of system components. Before automated support can be provided to detect and react to information assurance attacks, some *model* of the system is needed to support *detection* of attack situations, *analysis* of response options, and *execution* of selected responses. A current approach for large-scale system modeling assumes that the system can be *decomposed* into a set of components which are systems in their own right so that the system being studied can be analyzed as a composed *System of Systems* (SoS).

Military operations rely upon structured planning and re-planning processes that produce a series of products that support comparison of current system state to estimates of "normal" system state. Among these products are: the Task Organization (which provides relations among Task Force (TF) elements), the Signal Annex (which provides relations between System Architecture hardware and software components), and the synchronization matrix (which relates expected unit activities to execution of key events in support of realization of the commander's concept of the operation). Unit movements and engagement operations are continuous and occur on different time and spatial scales but are normally approximated as a series of discrete events.

This paper presents a (somewhat) novel view of the information assurance modeling problem as one where detection of anomalous SoS behaviors should be viewed as a *mixed-signal* system identification problem where some of the system components contain feedback loops. The term mixed-signal refers to the fact that some system components can be modeled using discrete-event models while other components are appropriately modeled using continuous models. The detection problem is then to produce an *estimate of the state of the system* by analyzing signals from available sensors that sample the state of discrete and continuous components.

All of the authors are with the Information Technology and Operations Center, Department of Electrical Engineering and Computer Science, United States Military Academy, West Point, New York 10996. Phone: (845) 938-5563; email:DJ7833@usma.edu. The views expressed herein are those of the authors and do not purport to reflect the position of the United States Military Academy, the Department of the Army, or the Department of Defense

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	6/6/2000	Research Paper 6/6/2000

4. TITLE AND SUBTITLE
Performance Modeling of AFATDS and Other Applications: Implications for Information Assurance and Security

5. FUNDING NUMBERS

6. AUTHOR(S)
James, John R.; Ragsdale, Dan; Schafer, Joseph; Presby, Tim

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
IEEE

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
IATAC
3190 Fairview Park Drive
Falls Church, VA 22042

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(Maximum 200 Words)*

ABSTRACT: Planning of complex activities is a deliberative process and automation support for re-planning activities should provide for cognitive modeling of the planning process. This paper takes the position that the cognitive model should contain details of the domain being supported and, especially for support of on-line re-planning, knowledge of the system implementation architecture – including performance modeling of the implementation architecture. We discuss these thoughts in some detail and provide an overview of a test bed framework being implemented to perform experiments on the validity of this approach. In particular, we are interested

14. SUBJECT TERMS
IATAC Collection, information assurance, metrics, performance modeling, distributed computing, latency, cognitive modeling, pattern recognition

15. NUMBER OF PAGES
7

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

Many control system engineers would not consider such a view as particularly novel, particularly those who have been involved in the *hybrid-system* efforts of the past ten years where this problem has been studied in detail for control system problems. However, system engineers of military command and control systems normally model command and control systems using discrete-event models only, assuming that any continuous portions of the problem have been adequately approximated by discrete-event models. This paper argues that information assurance problems should be modeled using a control systems view of the composed SoS and provides an overview of tools and techniques being incorporated into a test bed that applies this view.

II. Organization

This paper presents two related notions: (1) higher-level, relatively slow decision support systems can benefit from treating (i.e. modeling and identifying) feedback control properties of relatively fast system processes, and (2) Information Operations is a category of decision support systems that requires explicit treatment of the attack detection problem as a mixed-signal identification problem. Such a view of large-scale systems is a *control system view* since the fundamental characteristic of control system science is the study of feedback loops. The paper will (1) assert that the Information Assurance vulnerability and survivability assessment problem is a "system of systems" problem containing feedback loops, (2) discuss *detecting* Information Operation attacks as a mixed-signal system identification problem, (3) review several current design environments which support a "system of systems" approach, and (4) discuss ideas on a test bed framework for conducting experiments to achieve on-line detection and reaction to Information Assurance attacks.

III. The Information Assurance Vulnerability/Survivability Problem

Use of reference architectures for component-based design and analysis of large-scale systems has become fairly widespread. Considering major system components as systems in their own right has led to the characterization of their composition into the implementation architecture of the overall system as the "system-of-systems" problem. The approach taken here is to consider the information assurance problem as a "system-of-systems" problem and also to consider the components of the problem domain models and architectures as containing feedback loops.
As enterprises rely more heavily on the benefits of electronic commerce, the problems associated with security of proprietary data has become a major issue. Recently, the United States, represented by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) has concluded an international agreement on assessing the status of information system security, the Common Criteria [17, 18]. Current DoD guidance on assessing the status of information system security is found in [19]. A discussion of the importance of information operations to critical DoD command and control systems and also recommendations for improving the status of information systems security is found in [16]. A critical observation contained in [16] is that an acceptable level of security is driven by a ***risk assessment*** in which a perfect security solution is recognized as unattainable while an ***80% solution*** will normally be acceptable. A similar recognition of the need for the information security process to be driven by a *risk assessment* is formally included in the Common Criteria discussed in [18, 19]. Commanders need a solution for achieving a level of trust that information system components are functioning properly and meeting the needs of the unit.
Adaptive network security is advocated by Internet Security Systems [13], a prominent provider of commercial products for network security, as a necessary approach for securing commercial enterprise networks against malicious attacks. ISS recommends a Detect, Monitor, Respond sequence for managing network attacks. Since military communication architectures are deliberately designed to change over time, degradation and enhancement of network information processing capability over time will be a characteristic of unit operations. Consistent with the discussion of the preceding paragraph, a unit's ability to *detect, monitor, and respond* to IO attacks should be based on: a ***risk assessment*** of unit vulnerabilities, a deliberate decision concerning an ***acceptable level of risk*** [20], and methodologies to achieve that level of risk in unit information systems.
For example, a detect, monitor and respond capability is a necessary element of the Autonomous Information Assurance [11] project of the Defense Advanced Research Projects Agency (DARPA). The AIA project envisions a reactive capability to respond to an IO attack (see Figure 1) predicated on an ability to estimate the current state of the battlefield processes being monitored.

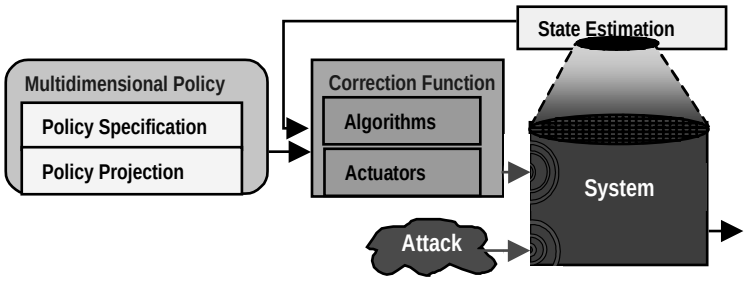


Figure 1. Feedback control concept for Autonomic Information Assurance

Thus, IO process analysis is necessarily preceded by an ability to *identify* normal current system architecture activities, and then enabled by an ability to *detect* new or previously-encountered anomalous activities, *monitor* anomalous activities, and *respond* to IO attacks. Following the reasoning presented in [21] the partitioning of the overall system into smaller system components is assumed to require consideration of feedback loops present in system processes. This is not a new position. Indeed, the component aggregation and disaggregation problem has been repeatedly studied [2, 3, 4, 11, 15]. A good summary is found in [39]. Furthermore, the problem domain of at

least one of the system components (e.g. the target engagement problem or the quality-of-service-based bandwidth allocation/reallocation problem) is assumed to be a "mixed-signal" problem. The Modelica language development effort in Europe now has a commercial implementation for control systems, as do the VHDL-A and Verilog languages used for electronic design and implementation. However, the emphasis on explicit modeling of system communication components in [12] is certainly different than many large-scale systems modeling efforts. Moreover, the range of system dynamics, together with explicit support for adapting goals and methods of the higher-level control plan is, if not unique to the military problem domain, certainly not the problem normally encountered in mixed-signal control analysis and design. As with other hybrid control problems, the central, enduring difficulty has remained that, while we are able to simulate the composed problem, we are unable to discover all failure modes of complex, adaptive systems whose dynamics are approximated by the composed models. We are, thus, able to reliably react to known failure modes but are unable to guarantee a controlled response to undetected failure modes.

For an analysis framework, prudent resource management (as well as practical engineering concerns) requires that minimal required effort be expended to achieve "close-enough" models of system dynamics, similar to the philosophy of Professor Lotfi Zadeh's soft-computing effort [24]. A major hurdle in such an endeavor to reactively determine what is "close enough" is to determine what is "timely enough". In this regard, the ideas of E. Douglas Jensen [20] concerning "soft-real-time" system analysis as a necessary compliment to "hard-real-time" analysis are especially appropriate. Finally, an analysis framework for IO must be capable of capturing the military decision-making process that begins with receipt of a mission, continues to analysis of alternative courses to action to accomplish the mission, generates an operations plan to execute the chosen course of action, and monitors the execution of the plan, re-planning as necessary [21-23, 42-45]. For Army operations, the timeliness [20] of Battlefield Operating Systems is dynamically determined by the synchronization matrix produced during the military decision-making process (MDMP) [27].

IV. Detecting Information Operations Attacks

Information Operations are those operations which affect the cognitive processes of command or the systems that support these processes. Information operations can be offensive or defensive. The Army has categorized expected threats to information systems (Figure 2) by level of hostility, adversaries, and adversary options [5]. Commanders have used Defense Condition (DEFCON) notices for many years to alert units to changes in levels of hostility. Recently, Information Condition (INFOCON) levels have been established to enable commanders to alert units to changes in likelihood of information operation attacks which correspond to the changes in the levels of hostility depicted in Figure 2.

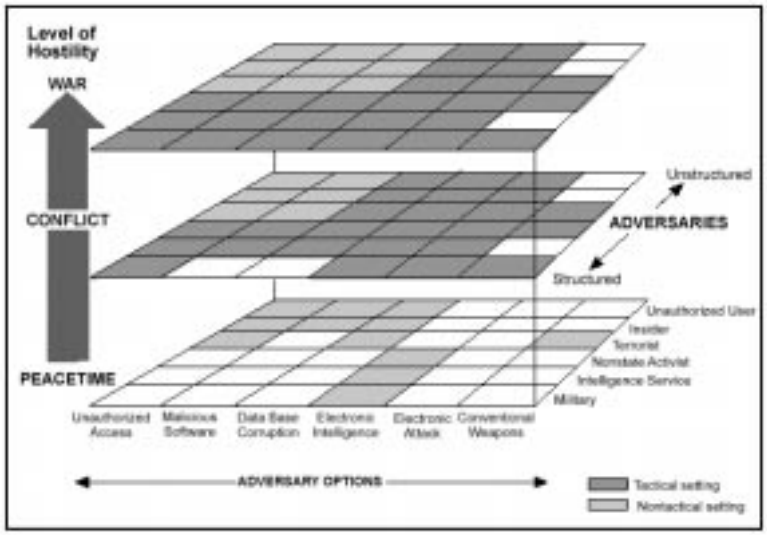


Figure 2. Threats to Information Systems

Identification of the major components of a large-scale, distributed system is a daunting task. The approach taken here is to leverage existing knowledge of the problem domain to greatly simplify that task by breaking the overall problem down into more manageable sub-problems. Consider the problem domain to be the *detection* of Information Operation attacks directed against the First Digitized Division (FDD) to be fielded by the U.S. Army in the next eighteen months. A key feature of the FDD is implementation of a tactical local area network (LAN) to support Information Dominance of friendly forces over opposing forces. The discussion below of the Information Operation detection problem simply takes advantage of the tremendous effort being expended by the Army to apply the concepts of product-line, system-of-systems architectures and reusable components (e.g. see [5, 6, 7, 8, 9, 10]). The Army Enterprise Architecture (AEA) [8] provides guidance on the digitization of Army tactical and installation information systems. The AEA directs construction of a single Army information system architecture with three views: *Operational, System, and Technical* (Figure 3). Thus, we expect to observe in fielded implementation architectures (i.e. the hardware and software present in units vary according to *System Architectures* for specific units) a ***"normal"*** flow of information corresponding to the battlefield processes of a given unit (i.e. the input-output characteristics correspond to the *Operational Architecture* specified for the unit) which complies with the implementation standards required for the signal being observed (i.e. the transmission characteristics comply with the *Technical Architecture* of the unit being observed). The AEA provides the framework for life-cycle system management of Army information technology systems, including Army Command, Control, Communications, Computers, and Intelligence (C^4I) systems.

Our identification problem is then to filter the observed signals into appropriate sets of data for the unit being analyzed and to compare known patterns for separable components to patterns observed in the data being analyzed. Metrics are needed to determine closeness of observed patterns to expected patterns. Anomalous activity is then indicated (detected) when differences exceed some user-determined threshold.

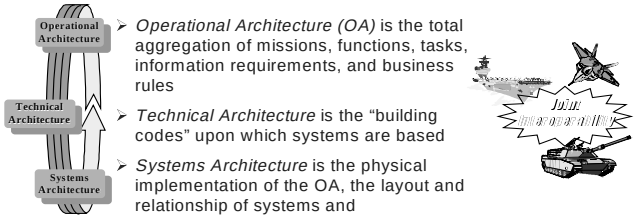


Figure 3. Army Enterprise Architecture

Each of the divisional *system architectures* will be different and will change as new equipment is introduced. As each division deploys to conduct operations, each operations order (OPORD) executed by units will comply with the *operational architecture* of the AEA with changes as needed to accommodate current circumstances. The *technical architecture* will change slowly to accommodate new technologies. Thus, the majority of the new work is to create an analytical framework for analysis of the Army IO problem as a "system of systems" problem of composition of dynamical decision components which change over time. For example, consider the issues surrounding detecting and reacting to Information Operation attacks during a battalion (Task Force XXI) deliberate attack. Two documents produced either separately during the MDMP or as part of an Operations Order (OPORD) are the Task Organization and the Signal Annex. The Task Organization provides the hierarchy of units conducting the operation and the Signal Annex provides the description of the mobile, fixed, and local area-network communications used during the operation.

A test bed is being constructed that will be able to use results from simulation models such as the Corps Battle Simulation (CBS – which requires extensive user participation), Eagle (which has extensive support for generation of attrition-based simulation from a commander's concept of the operation), and CASTFOREM (which requires extensive preparation of a scenario for high-fidelity simulation of attrition-based outcomes). Each of these simulations, and others, provide command and control message traffic (e.g. verbal reports and orders) and situational awareness data traffic (e.g. position, status and activity data) corresponding to an operational scenario. The test bed we are constructing will run as a set of applications on the Information Warfare Analysis and Research (IWAR) laboratory and will use a set of intelligent agents to model unit activities and detect information operation attacks.

The Task Organization and Signal Annex network knowledge from simulated operations will be used to apply evaluation technologies to enable the agents to make an assessment of whether the status of the operation execution is normal (Green), somewhat abnormal (yellow), or definitely anomalous (red).

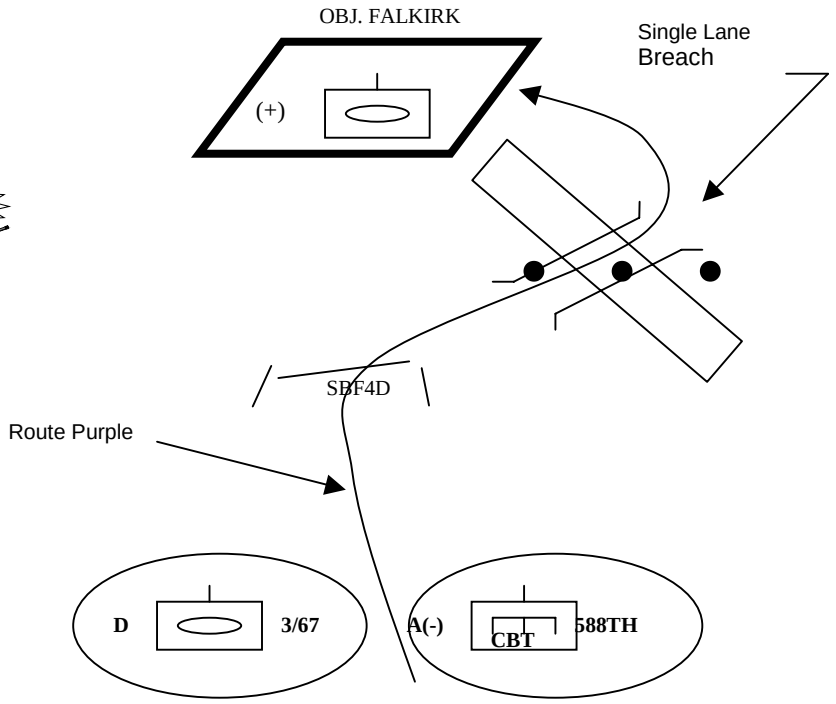


Figure 4. Excerpt of Scenario

An initial set of activities for the agents will be to determine the center of mass of the units in the Task Force XXI organization using the situational awareness (SA) output of an operation. We intend to begin with a subset of a maneuver concept such as that outlined in [29]. Figure 4 provides a visual summary of a portion of a typical scenario. The unit *mission* is to sieze objective Falkirk. The sequence of events depicted in Figure 4 represents a critical sequence of battlefield activities necessary for successful execution of the commander's *Concept of the Operation* to achieve the commander's *intent* stated in the unit OPORD. The excerpt reflects the commander's concept that Team Dawg (Armor) will advance along Route Purple to occupy position Support By Fire 4D (SBF4D) and provide covering fire while Task Force 588TH (Combat Engineer) clears a single-lane breach of a minefield obstacle in front of Objective Falkirk. Not shown is the subsequent attack by Team Dawg, Team Cobra, and Team Bushmaster.

As indicated in [29], "The 'TF-Assault' decisive point of action was when the TF Commander instructs Teams Dawg, Bushmaster, and Cobra to assault Objective Falkirk. The 'CO-SBF4D' and 'PLT-Breach' decisive points of action were when "Dawg is set at SBF4D and the TF 588th Combat Engineers have breached the obstacle. . ." Army XXI will enjoy improved situational awareness through use of improved radios to transmit command and control messages and use of Future Battle Command – Brigade and Below (FBCB2) equipment on vehicles to automatically

determine and transmit vehicle location as well as vehicle status and activity.

A few comments are appropriate at this point concerning how "timeliness" is itself a variable in military operations. The vignette of Figure 4 is part of a battalion-level operation that will take less than two hours to execute. During that time, the company-level sequence of activities between the 'CO-SBF4D' and 'PLT-Breach' events will take less than a half-hour to execute. Platoon and weapon system movement activities may take a few minutes. Calls for indirect fire (artillery and missiles) may take thirty seconds to execute while direct-fire engagements may only take a few seconds. Throughout the operation, the battalion, company, platoon, and fire unit leadership may dynamically replan execution of the OPORD for their levels of command and time frames for execution as conditions change.

Certainly the majority of command and control activities are keyed on events and discrete-event models are sufficient to capture the complexity of those events. Consider in slightly more detail two functional areas that require mixed-signal analysis: engagement of multiple targets by multiple weapons platforms and dynamic bandwidth allocation. Engagement of multiple targets by multiple weapons platforms is a difficult problem where detection, identification, prioritization, selection, engagement, and re-engagement tasks must be made under severe time and uncertainty constraints. A mixed-signal model of the problem is developed in [30].

A significant issue during preparation for and execution of Operation Desert Storm was the fact that available bandwidth was allocated (reserved) on a priority basis to command and control entities concerned with control of maneuver and engagement activities. This was true throughout the preparation and execution phases of the operation even though the engagement and maneuver operations only required use of the reserved bandwidth for a small fraction of the timeframe when maneuver and engagement operations were conducted and even less during the preparatory time. Fielding of the Joint Tactical Radio System (JTRS) and Warfighter Information Network – Terrestrial (WIN-T) will enable dynamic allocation and reallocation of bandwidth based on priority of use and quality of service. In the interim, the Near-Term Digital Radio (NTDR) and enhancements to the existing Mobile Subscriber Equipment (MSE) will support initial experiments with dynamic bandwidth allocation. Even in the short scenario outlined above, the utility of such a bandwidth control capability can be seen when considering the intermittent loss of communications with maneuvering units due to terrain masking of signal transmission and loss of communications or computing elements due to equipment failure or enemy action. OPNET [31] is a widely-used tool for modeling network communication devices. Another tool is available for estimating connectivity between mobile platforms that require line-of-sight for radio communications connectivity.

As indicated above the test bed will initially simply filter available message traffic and situational awareness data to create templates of unit movement and communication activities keyed to OPORD events. Specifically, we will support analysis of such activities as the processes that determine the time at which the event "CO-SBF4D" occurs ($T_{CO\text{-}SBF4D}$) and the time at which the event "PLT-Breach" occurs ($T_{PLT\text{-}Breach}$). Using the Situational Awareness (SA) traffic to create such templates is the first step in being able to link sensed unit activities to the commander's Concept of the Operation.

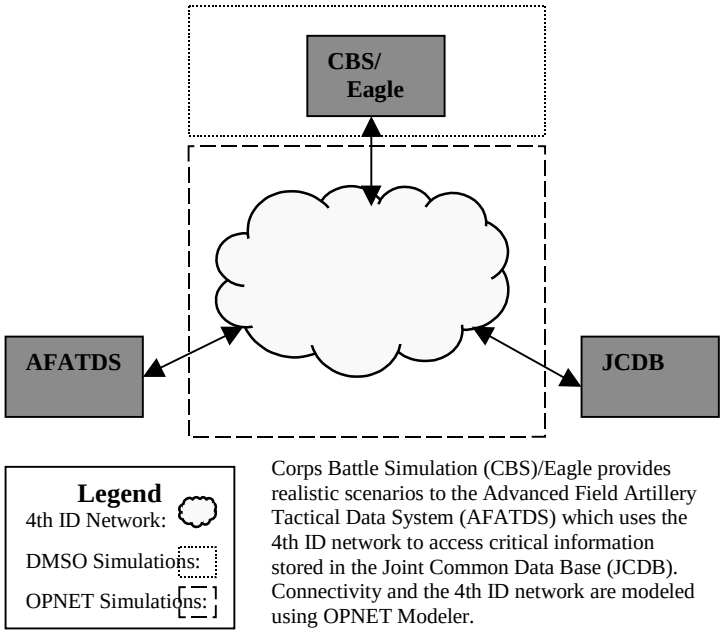
For larger units, a Synchronization Matrix (Execution Matrix) is constructed in the final stages of the Military Decision Making Process (MDMP) development of OPORDs and indicates unit activities in support of executing critical phases of the Commander's concept. The Fire Support Plan is one of the key plans that support construction of the synchronization matrix. Another planning product that is used in detailed planning of executing the concept of the operation is the Operational Schedule (OPSKED). The OPSKED and Fire Support Plan contain brevity codes that reference specific pre-planned target concentrations during key events in synchronization of phased maneuvers by maneuver elements and fire support activities by fire support elements (such as suppression of enemy activity in Objective Falkirk while engineer elements are clearing the minefield and subsequently while Team Dawg moves through the breech in the minefield.

V. Test Bed Framework

The activities described above provide a required few "first steps" for agents to access and interpret information flowing from scenarios implemented on force-on-force, attrition-based model of combat operations. Similarly, preliminary analysis of any operation is necessary to enable agent-based detection of operations activities that are anomalous to those expected to be present in executing the commander's concept of the operation.

Additionally, analysis of the set of anomalous events to make an assessment of whether the status of the execution is normal (Green), somewhat abnormal (yellow), or definitely anomalous (red) will require the agents to have a deeper understanding of what range of deviation from "normal" is expected before the activity becomes "abnormal" or "anomalous". For simulated activities, message delay or loss can be used to simulate IO attacks. Such results would be at the application layer level of the AEA Technical Architecture since this is the level at which message traffic occurs. To make the assessment of anomalous activity "real", the simulated environment should be made as close as possible to the actual environment of the "system of systems" that makes up the Army XXI *Systems Architecture*. The Next Generation Performance Model (NGPM) of the Communication-Electronics Command (CECOM) Research Development and Engineering Center (RDEC) is being implemented using extensions to OPNET modules to provide the ability to model the Force XXI environment at the network level. We intend to use the NGPM to support assessments at the platform layer or network layer [9]. For example, OPNET could be used to model the Army tactical local area network

(LAN) [7] or the joint task force network [25] and assess network-level attacks against command and control systems such as the Advanced Field Artillery Tactical Data System



(AFATDS). The concept is summarized in Figure 5.

Figure 5. Test Bed Concept

Future command and control systems of Joint Task Forces (JTFs) will be a network of applications running in a distributed environment. These applications, such as AFATDS, will depend upon timely distribution of data stored in the Joint Common Data Base. This project aims to create an initial capability for conducting metrics-based experiments concerning performance of distributed applications under a variety of operational conditions. The test bed will leverage Army investments in Defense Modeling and Simulation Office (DMSO) compliant simulations such as the Corps Battle Simulation (CBS) and Eagle. The test bed will also use Army-developed models of the 4th ID network and the OPNET Modeler commercial network-modeling tool to achieve a capability to evaluate performance characteristics of distributed applications. Implementation of the test bed will depend upon use of a new capability for OPNET Modeler, the Application Characterization Environment (ACE) module. The PM FATDS has provided the ITOC with an AFATDS system. The CBS/Eagle simulations, 4th ID network simulation, and JCDB system will be running on separate computers in the IWAR laboratory. OPNET has a module that implements the DMSO High Level Architecture (HLA) which supports explicit control of synchronization of distributed applications using timed events. We expect to answer questions such as: "What is the data base access time for AFATDS to obtain item X from the JCDB?", or "What is the change in the data base access time for AFATDS to obtain item X from the JCDB when change Y occurs in the network?"

VI. Design Environments for Nonlinear Systems Identification

Most large, complex automation systems (e.g. finance, transportation, maintenance) are built and reliably maintained while applying an underlying assumption that each individual component is independent of all other components (i.e. the next state and output of each component depends only on the current component state and the current input to the component). However, for a large class of systems, the presence of feedback loops among sets of system components invalidates the independence assumption for those coupled components and, therefore, reliable system construction requires explicit identification of process feedback loops and their use in the system development process. Also, for large systems, event-based decisions make the models highly non-linear, with possible emergent dynamics dependant upon choices made by humans-in-the-loop. One widely-used set of nonlinear models for approximating military systems is the Lanchester-based attrition models [15] used for estimating battle outcomes. Actual warfare is considerably more nonlinear than the relatively well-behaved Lanchester equations which are normally the primary continuous-system component of an event-based military systems simulation environment. The discussion found in [15] is an excellent summary of the challenges present in aggregation and disaggregation of military models. The problem of nonlinear, mixed-signal system identification occurs widely in control system science and engineering [1-4]. Such models can lead to chaotic system state and chaotic system response. While most applications seek to avoid the conditions for onset of chaos, others have discovered that physical system data (especially in biological sciences) exhibit chaotic behavior. While electronics engineers continue to use the mixed-signal term, in the past ten years control engineers have began to refer to mixed-signal problems as ***hybrid systems*** problems [31].

The web page of the IEEE Control System Society (CSS) Technical Committee on Hybrid Dynamical Systems [50] has links to several active research groups and also to some computer packages for modeling hybrid systems. In addition, environments at the University of California at Berkeley [3] and Georgia Tech [2] support efforts in a Software-Enabled Control (SEC) initiative funded by the US Department of Defense. The SEC sites discuss use of software-enabled control to control autonomous air vehicles.

The Spatial Aggregation Language (SAL) has been developed by Feng Zhou to support analysis and design of hybrid systems [4]. The approach is being investigated at XEROX Palo Alto Research Center (PARC) as an environment for complex system design.

The Modelica language [34] has been under development for several years in Europe and now has a commercial implementation for control systems, as do the VHDL-AMS (now IEEE Standard 1076.1) [35] and Verilog [36] languages used for electronic design and implementation. However, the emphasis on explicit modeling of system communication components in [12] is certainly different

than many large-scale systems modeling efforts. Moreover, the range of system dynamics, together with explicit support for adapting goals and methods of the higher-level control plan is, if not unique to the military problem domain, certainly not the problem normally encountered in mixed-signal control analysis and design.

The Discrete Event Simulation System (DEVS) developed by Professor Bernard Ziegler has been widely used for simulation of military systems and has recently been modified to be compliant with the Department of Defense (DoD) High Level Architecture (HLA). Neither HLA or DEVS has explicit support for hard-real-time systems simulation but both have been used for soft-real-time-simulation. Several engineering design groups have been working on a system-level language that supports partitioning of functionality between hardware and software modules [36].

As with other hybrid control problems, the central, enduring difficulty has remained that, while we are able to simulate the composed problem, we are unable to discover all failure modes of complex, adaptive systems whose dynamics are approximated by the composed models. We are, thus, able to reliably react to known failure modes but are unable to guarantee a controlled response to undetected failure modes. Thus, similar to the development of the flyball governor for steam engines and the electronic feedback amplifier for telephone lines, engineers have again progressed to the point of building useful and (normally) reliable systems whose performance capabilities exceed the analytical capabilities of current theoretical approaches to predict, verify and validate system performance.

VII. REFERENCES

[1] Zadeh, L. A., "The Evolution of Systems Analysis and Control: A Personal Perspective", *IEEE Control Systems*, Vol. 16, No. 3. pp 95-98, 1996.

[2] Georgia Tech Software-Enabled Control (SEC) web page: http://controls.ae.gatech.edu/projects/sec/

[3] U. C. Berkeley Software-Enabled Control (SEC) web page: http://sec.eecs.berkeley.edu/

[4] Xerox PARC Spatial Aggregation Language (SAL) web page: http://www.parc.xerox.com/spl/members/zhao/stanford-cs329/sal-doc/index.html

[5] Headquarters, Department of the Army, FM 100-6, Information Operations, August, 1996.

[6] Headquarters, Department of the Army, FM 100-5, Operations, May, 1997.

[7] Headquarters, Department of the Army, FM 24-7, Tactical Local Area Network (LAN) Management , October, 1999.

[8] Office of the Director of Information Systems for Command, Control, Communications, and Computers (ODISC4), The Army Enterprise Architecture Master Plan, Vol.1, 30 September, 1997.

[9] Office of the Director of Information Systems for Command, Control, Communications, and Computers (ODISC4), Joint Technical Architecture –Army, Version 6, May 8, 2000.

[10] Defense Information Systems Agency (DISA), Defense Information Infrastructure – Common Operating Environment (DII-COE) Integration and Runtime Specification (I&RTS),Version 4, October, 1999.

[11] DARPA Autonomous Information Assurance Program web page: http://web-ext2.darpa.mil/iso/IA&S/IASPIP990811Final.html

[12] James J. and R. McClain "Tools and Techniques for Evaluating Control Architecture," Proceedings of the 1999 IEEE International Symposium on Computer Aided Control System Design, Kohala Coast-Island of Hawai'i, Hawai'i, USA, August 22-27, 1999.

[13] Internet Security Systems, Adaptive Network Security Handbook, http://www.iss.net/.

[14] Benveniste, A and K. Åström " Meeting the Challenge of Computer Science in the Industrial Application of Control: An Introductory Discussion to the Special Issue" *IEEE Transactions on Automatic Control*, Vol. 38,pp.1004-1010, 1993.

[15] Davis, Paul K, Aggreggation, Disaggregation, and the 3:1 Rule in Ground Combat, RAND Report MR-638-AF/A/OSD, http://www.rand.org/publications/MR/MR638

[16] Committee to Review DOD C4I Plans and Programs of the Computer Science and Telecommunications Board of the Commission on Physical Sciences, Mathematics, and Applications of the National Research Council, *Realizing the Potential of C4I - Fundamental Challenges*, **National Academy Press,** Washington, D.C. 1999

[17] Depart of Defense Instruction Number 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)", 30 December 1997.

[18] Troy, Eugene F., NIST-ITL, "Common Criteria: Launching The International Standard," http://csrc.nist.gov/cc/info/cc_bulletin.htm 24 November 1998.

[19] Common Criteria for Information Technology Security Evaluation, Common Criteria Version 2.1 / ISO IS 15408 http://csrc.nist.gov/cc/ccv20/ccv2list.htm August 1999.

[20] Jensen, E. Douglas, "Real-Time for the Real World", http://www.real-time.org/no_frames/mitre.htm

[21] JCS Publication 1, "Joint Warfare of the Armed Forces of the United States", 10 January 1995.

[22] JCS Publication 3-0, "Doctrine for Joint Operations", 1 February 1995.

[23] JCS Publication 5-0, "Doctrine for Planning Joint Operations", 13 April 1995.

[24] Berkeley Initiative in Soft Computing, http://www.cs.berkeley.edu:80/projects/BISC/bisc.welcome.html

[25] Department of the Army, Field Manual FM 100-14, "Risk Management," Washington, DC, 23 April1998.

[26] Department of the Army, Field Manual 101-4 Multiservice Procedures for Joint Task Force Information Management JTF-IM, MRCP 6-23A, NWP 3-13.1.16, AFTTP(I) 3-2.22, April 1999.

[27] Department of the Army, Field Manual FM 101-5, "Staff Organization and Operations, " Washington, DC, June 1996

[28] Department of the Army, Field Manual FM101-5-1. MCRP 5-2A, "Operational Terms and Symbols". Washington, DC, 30 Sept 1997.

[29] Department of the Army, Field Manual FM101-5-2., "U. S. Army Report and Message Formats" Washington, DC, 5 March 1999.

[30] anonymous, "Assessing Task Force XXI (TF XXI) Digitization - Section 1: Fort Hood company/battalion attack," undated, unclassified summary.

[31] Kohn, W., John James, Anil Nerode, and Jin Lu, "Multiple-Agent Hybrid Control Architecture for the Target Engagement Process (MAHCA-TEP) *Technical Background, Simulation Requirements, and Engagement Model,"* 25 August, 1994. Intermetrics, Inc. Technical Report delivered to Odyssey Research, Inc. under the DARPA DSSA program, administered by Dr. Norm Coleman, US Army ARDEC.

[32] MIL3 – Third Millennium Technologies, OPNET – Decision Support Software for Networks and Applications, http://www.mil3.com/

[33] IEEE Control System Society Technical Committee on Hybrid Dynamical Systems, http://www.nd.edu/~lemmon/hybrid/index.html

[34] Modelica - A Unified Object-Oriented Language for Physical Systems Modeling http://www.dynasim.se/modelica.html

[35] VHDL-AMS, http://vhdl.org/, http://www.vhdl-ams.com/

[36] Verilog Hardware Description Language, http://www.cadence.com

[37] System-Level Design Language, http://www.inmet.com/SLDL/

[38] James, J. R., "Modeling Information Assurance Dynamics: An Initial Concept", DRAFT, May, 2000.

[39] Otter, M., and F.E. Cellier (1995), Software for Modeling and Simulating Control Systems, The Control Handbook (W.S. Levine, ed.), CRC Press, Boca Raton, FL, pp.415-428.